# *On Ternary Substitution-Groups of Finite Order which leave a Triangle unchanged.*

By H. Maschke.

In his papers, "Sur les équations différentielles linéaires à intégrale algébrique,"* and "Sur la détermination des groupes d'ordre fini contenues dans le groupe linéaire,"† C. Jordan has enumerated all those ternary linear substitution-groups whose order is a finite number. Three of these groups, being of special interest, viz. one group of order 60, isomorphic with the icosahedron-group,‡ one of order 216, the so-called Hessian-group,§ and one of order 168,‖ have been thoroughly investigated. But nothing has been done as yet with regard to those apparently simple ternary groups whose substitutions are given by formulæ of this kind:

$$z_1' = az_i, \quad z_2' = bz_k, \quad z_3' = cz_l,$$

where $a$, $b$, $c$ are roots of unity and $i$, $k$, $l$ in some order equal to 1, 2, 3.

It seems to be appropriate to name substitutions of this type "*monomial*" substitutions, and groups containing only monomial substitutions "*monomial groups.*"

In the following a first step towards a complete treatment of these ternary monomial groups will be made, viz. the investigation of those groups "$G$" whose substitutions are generated by the following two monomial substitutions:

$$S: \left.\begin{aligned} z_1' &= z_2, \\ z_2' &= z_3, \\ z_3' &= z_1, \end{aligned}\right\} (1), \qquad T: \left.\begin{aligned} z_1' &= a_1 z_1, \\ z_2' &= a_2 z_2, \\ z_3' &= a_3 z_3, \end{aligned}\right\} \quad (2)$$

* Borchhardt's Journal, Bd. 84.

† Atti della Reale Accademia di Napoli, 1880.

‡ F. Klein, Math. Ann., Bd. 12, p. 529; Icosaëder, p. 213 ff.

§ A. Witting, Dissertation, Göttingen, 1887, p. 28 ff.; H. Maschke, Math. Ann., Bd. 33, p. 324.

‖ F. Klein, Math. Ann., Bd. 14, p. 144; Bd. 15, p. 265. Klein-Fricke, Modulfunctionen, I, p. 692 ff.

where $a_1$, $a_2$, $a_3$ are roots of unity. $T$ may also be written in this form:

$$\left.\begin{aligned} z_1' &= e^{\frac{2k_1\pi i}{m_1}} z_1, \\ z_2' &= e^{\frac{2k_2\pi i}{m_2}} z_2, \\ z_3' &= e^{\frac{2k_3\pi i}{m_3}} z_3, \end{aligned}\right\} \tag{3}$$

$k_1$, $k_2$, $k_3$ and $m_1$, $m_2$, $m_3$ being integers.

The determinant of substitution $S$ is 1. We impose the same condition also on substitution $T$, viz. $a_1a_2a_3 = 1$, or

$$\frac{k_1}{m_1} + \frac{k_2}{m_2} + \frac{k_3}{m_3} = n, \tag{4}$$

where $n$ is any integer.

## §1. *The Invariant Forms of G.*

We may assume $k_1$ to be prime to $m_1$, $k_2$ to $m_2$, $k_3$ to $m_3$. Let $R$ be the greatest common divisor of $m_1$ and $m_2$, so that

$$m_1 = p_1R, \quad m_2 = p_2R, \tag{5}$$

then $p_1$ and $p_2$ will be prime to each other and

$$p_1p_2R = P \tag{6}$$

the least common multiple of $m_1$ and $m_2$. But equation (4) shows that $P$ is divisible also by $m_3$, therefore *$P$ is the period of $T$.*

It follows from $S$ that in every *invariant form* of $G$—i. e. a homogeneous integral function of $z_1$, $z_2$, $z_3$ which remains absolutely unchanged when the three variables are operated upon by the substitutions of $G$—only terms of these three types are admissible:

Type I : $z_1^\alpha + z_2^\alpha + z_3^\alpha$,
Type II : $z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + z_3^\alpha z_1^\beta$,
Type III: $z_1^\alpha z_2^\beta z_3^\gamma + z_2^\alpha z_3^\beta z_1^\gamma + z_3^\alpha z_1^\beta z_2^\gamma$.

We see at once that $z_1z_2z_3$ is invariant, or, spoken geometrically, that the triangle of reference remains unchanged. Hence every form of type III is reducible to a product of some power of $z_1z_2z_3$ into a form of type I or type II, and if in

type II we admit the value zero for $\alpha$ or $\beta$, we see that forms of type I may also be discarded. So we have the following theorem:

*Every invariant form of $G$ is an integral function of $z_1z_2z_3$ and of forms $z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + z_3^\alpha z_1^\beta$* ($\alpha$ and $\beta$ being positive integers or zero).

We now have to find the conditions that $z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + z_3^\alpha z_1^\beta$ remains invariant with regard to $T$.

If we apply $T$ to $z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + z_3^\alpha z_1^\beta$ and put this expression equal to the transformed expression, we see that the following three equations must be satisfied:

$$\left.\begin{aligned} \frac{\alpha k_1}{m_1} + \frac{\beta k_2}{m_2} &= \lambda\ , \\ \frac{\alpha k_2}{m_2} + \frac{\beta k_3}{m_3} &= \lambda_1, \\ \frac{\alpha k_3}{m_3} + \frac{\beta k_1}{m_1} &= \lambda_2 \end{aligned}\right\} \tag{7}$$

($\lambda$, $\lambda_1$, $\lambda_2$ integers).

Substituting, now, the value of $\frac{k_3}{m_3}$ taken from (4) into (7), we obtain

$$\left.\begin{aligned} \frac{\alpha k_1}{m_1} + \frac{\beta k_2}{m_2} &= \lambda, \\ \frac{\alpha k_2}{m_2} - \beta\left(\frac{k_1}{m_1} + \frac{k_2}{m_2}\right) &= \mu \end{aligned}\right\} \tag{8}$$

($\lambda$ and $\mu$ integers).

Adding together these two equations (8) and combining the result with (4), we obtain the third equation (7), which therefore may be omitted.

Let now $c$ be the greatest common divisor of $k_1$ and $k_2$, so that

$$k_1 = cx_1,\ k_2 = cx_2, \tag{9}$$

then $\lambda$ and $\mu$ must be divisible by $c$ because $k_1$ is prime to $m_1$ and $k_2$ to $m_2$. Changing the signification of $\lambda$ and $\mu$, we have these two equations

$$\begin{aligned} \frac{\alpha x_1}{m_1} + \frac{\beta x_2}{m_2} &= \lambda, \\ \frac{\alpha x_2}{m_2} - \beta\left(\frac{x_1}{m_1} + \frac{x_2}{m_2}\right) &= \mu \end{aligned}$$

($\lambda$ and $\mu$ integers).

Multiplying by $m_1 . m_2$ and substituting the expressions (5), we obtain

$$\left.\begin{aligned} \alpha x_1 p_2 + \beta x_2 p_1 &= \lambda p_1 p_2 R, \\ \alpha x_2 p_1 - \beta (x_1 p_2 + x_2 p_1) &= \mu p_1 p_2 R, \end{aligned}\right\} \tag{10}$$

and in these equations $x_1$ is prime to $x_2$ and to $p_1$, $x_2$ to $x_1$ and $p_2$, $p_1$ to $p_2$. It follows, therefore, from the first of these equations that $\alpha$ is a multiple of $p_1$, $\beta$ a multiple of $p_2$, and then from the second that $\alpha$ is a multiple of $p_2$, and $\beta$ a multiple of $p_1$. Hence

$$\alpha = \alpha' p_1 p_2, \ \beta = \beta' p_1 p_2, \tag{11}$$

where $\alpha'$, $\beta'$ are two new integers. Substituting these values into (10), we may divide by $p_1 p_2$ and have

$$\begin{aligned} \alpha' x_1 p_2 + \beta' x_2 p_1 &= \lambda R, \\ \alpha' x_2 p_1 - \beta' (x_1 p_2 + x_2 p_1) &= \mu R, \end{aligned}$$

or, using the abbreviation

$$x_1 p_2 = p, \ x_2 p_1 = q, \tag{12}$$

$$\left.\begin{aligned} \alpha' p + \beta' q &\equiv 0 \pmod R, \\ \alpha' q - \beta' (p + q) &\equiv 0 \pmod R, \end{aligned}\right\} \tag{13}$$

where $p$ and $q$ are prime to each other.

Solving (13) with regard to $\alpha'$ and $\beta'$, we find

$$\left.\begin{aligned} \alpha' (p^2 + pq + q^2) &\equiv 0 \pmod R, \\ \beta' (p^2 + pq + q^2) &\equiv 0 \pmod R. \end{aligned}\right\} \tag{14}$$

Let now $t$ be the greatest common divisor of $p^2 + pq + q^2$ and $R$, so that

$$\left.\begin{aligned} p^2 + pq + q^2 &= st, \\ R &= rt, \end{aligned}\right\} \tag{15}$$

then it follows from (14),

$$\begin{aligned} \alpha' s &\equiv 0 \pmod r, \\ \beta' s &\equiv 0 \pmod r. \end{aligned}$$

But $r$ and $s$ have no common divisor, therefore

$$\alpha' = r\alpha'', \ \beta' = r\beta'', \tag{16}$$

where $\alpha''$ and $\beta''$ are again two new integers.

Substituting (16) into (13), we may divide by $r$ and obtain

$$\alpha'' p + \beta'' q \equiv 0 \pmod t, \tag{17}$$

$$\alpha'' q - \beta'' (p + q) \equiv 0 \pmod t, \tag{18}$$

and here $t$ *has no common divisor with* $p$ *and* $q$. This follows immediately from $p^2 + pq + q^2 = st$ and from $p$ being prime to $q$.

We now have to find the solutions of the congruences (17) and (18). For that purpose let us first treat congruence (17). Assign to $\alpha''$ any positive integral value. We may write

$$\alpha'' \equiv n \pmod{t}, \tag{19}$$

where $n < t$. Then we have

$$\beta'' q \equiv -np \pmod{t}. \tag{20}$$

Solve now the congruence

$$v.q \equiv -p \pmod{t}. \tag{21}$$

We know there will exist one and only one solution $v < t$. Denote this particular value by $v$. Then the general solution of (20) is

$$\beta'' \equiv nv \pmod{t}. \tag{22}$$

We have thus in (19) and (22) the most general solution of (17).

Let us substitute these values of $\alpha''$ and $\beta''$ into (18). We obtain

$$nq - nv(p+q) \equiv 0 \pmod{t}.$$

If $n = 0$, this congruence is satisfied. If $n \not\equiv 0$, we may divide by $n$ and multiply by $q$ (which is prime to $t$),

$$\therefore\ q^2 - vq(p+q) \equiv 0 \pmod{t}.$$

But $vq \equiv -p \pmod{t}$, hence (18) becomes

$$q^2 + pq + p^2 \equiv 0 \pmod{t},$$

which congruence is satisfied indeed according to (15). *The solutions* $\alpha''$ *and* $\beta''$ *of* (17) *satisfy therefore also* (18) *without any further restriction.*

It is evident that the general solution may also be obtained by first assuming some integral value for $\beta''$, i. e.

$$\beta'' \equiv n \pmod{t}. \tag{23}$$

Denoting the smallest positive root of the congruence

$$w.p \equiv -q \pmod{t} \tag{24}$$

by $w$, we have

$$\alpha'' \equiv nw \pmod{t}. \tag{25}$$

The values of $\alpha$ and $\beta$ are now given by (11), (16) and (19), (20) or (25), (23), viz.

$$\left.\begin{aligned}\alpha &= p_1p_2r(\lambda t + n),\\ \beta &= p_1p_2r(\mu t + n\nu),\end{aligned}\right\} \tag{26}$$

or

$$\left.\begin{aligned}\alpha &= p_1p_2r(\lambda t + n\omega),\\ \beta &= p_1p_2r(\mu t + n).\end{aligned}\right\} \tag{27}$$

Since $p_1p_2rt = p_1p_2R = P$—see equations (15) and (6)—we may also write

$$\left.\begin{aligned}\alpha &\equiv n.p_1p_2r \pmod P,\\ \beta &\equiv n\nu.p_1p_2r \pmod P,\end{aligned}\right\} \tag{28}$$

or

$$\left.\begin{aligned}\alpha &\equiv n\omega.p_1p_2r \pmod P,\\ \beta &\equiv n.p_1p_2r \pmod P,\end{aligned}\right\} \tag{29}$$

where $n$ stands for any positive integer $< t$, or zero.

We have thus obtained the following final result:

*All invariant forms of $G$ are integral functions of $z_1z_2z_3$ and of forms $z_1^\alpha z_2^\beta + z_2^\alpha z_3^\beta + z_3^\alpha z_1^\beta$, where $\alpha$ and $\beta$ are to be found by the following process: Find the greatest common divisor $R$ of $m_1$ and $m_2$, and put $m_1 = p_1R$, $m_2 = p_2R$, $p_1p_2R = P$. Divide the two numbers $k_1$, $k_2$ by their greatest common divisor and call the quotients $\varkappa_1$ and $\varkappa_2$. Denote $p_1\varkappa_2 = p$ and $p_2\varkappa_1 = q$. Let $t$ be the greatest common divisor of $R$ and the quadratic form $p^2 + pq + q^2$; put $R = rt$. Solve the congruences*

$$v q \equiv -p \pmod t \text{ and } wp \equiv -q \pmod t,$$

*then $\alpha$ and $\beta$ are given by formulæ* (28) *or* (29).

## §2. *The Quantities $v$, $w$ and $t$.*

In the following we shall always suppose $t > 1$. The case $t = 1$ will be treated separately under the head "special cases" in §4.

Let us multiply the congruence (21) by (24). We may then divide by $pq$, which is prime to $t$, and obtain

$$vw \equiv 1 \pmod t. \tag{30}$$

Multiplying now (21) and (24) by $p$ and $q$ respectively and adding together, we obtain

$$(v + w)pq \equiv -p^2 - q^2 \pmod t,$$

or, since $-p^2-q^2\equiv pq \pmod t$, see (15),

$$v+w\equiv 1 \pmod t.$$

But $v$ and $w$ are both supposed to be $<t$, hence we have

$$v+w=t+1. \tag{31}$$

Finally we deduce from (21) the two congruences

$$v^2q^2\equiv p^2 \pmod t,$$
$$-vq^2\equiv pq \pmod t,$$

and joining the identity $q^2\equiv q^2 \pmod t$, we obtain by addition

$$q^2(v^2-v+1)\equiv p^2+pq+q^2 \pmod t,$$

or

$$v^2-v+1\equiv 0 \pmod t. \tag{32}$$

In a similar manner we find

$$w^2-w+1\equiv 0 \pmod t. \tag{33}$$

Thus we have the following result: The two quantities $v$ and $w$ are roots of the quadratic congruence

$$\omega^2-\omega+1\equiv 0 \pmod t; \tag{34}$$

they are connected by the relations

$$v+w=t+1 \text{ and } vw\equiv 1 \pmod t.$$

The congruence (34) is not solvable for every integral value of $t$. But it is always solvable for those values of $t$ which occur in the present problem. It is shown in the Theory of Numbers* that the quadratic form $p^2+pq+q^2$ ($p$ and $q$ prime to each other) represents all those and only those numbers $N$ which are given by $p_1^{\lambda_1}.p_2^{\lambda_2}.p_3^{\lambda_3}\ldots.$ or $3p_1^{\lambda_1}.p_2^{\lambda_2}.p_3^{\lambda_3}\ldots.$ where $p_1, p_2, p_3\ldots.$ are prime numbers of the form $3h+1$. The number $t$, being a divisor of $p^2+pq+q^2$ is therefore also of the form $N$. The smallest possible values of $t$ are these: **1**, 3, 7, 13, 19, 21, 31, 37, 39, 43, 49, 57, 61, 67, 73, 79, 91, 93, 97, etc.

Let $v$ be some root of the congruence (34), then $w=t+1-v$ is also a root of the same congruence, and the relation $vw\equiv 1 \pmod t$ is satisfied too. If $t$ is of the form $p_1^\lambda$ or $3p_1^\lambda$, then the congruence (34) has only two roots, and these roots are to be taken as $v$ and $w$. The lowest value of $t$ for which (34) has more

---

* Dirichlet-Dedekind, Zahlentheorie, 1871, p. 165.

than two roots is $t = 91$. In this case we have the four roots 10, 17, 75, 82, and here either 10 and 82 or 17 and 75 may be taken as a system $v$, $w$.

Let us examine the case $v = w$. In this case we have from (31)

$$v = w = \tfrac{1}{2}(t+1),$$

and from (32),

$$(t+1)^2 - 2(t+1) + 4 \equiv 0 \pmod{t},$$

or

$$t^2 + 3 \equiv 0 \pmod{t},$$

hence $t = 3$, $v = w = 2$.

The two numbers $v$ and $w$ are therefore always distinct except in the case $t = 3$.

## §3. *Connection between the Invariant Forms.*

For further investigation of the invariant forms let us put

$$p_1 p_2 r = \mathfrak{H}, \tag{35}$$

$$z^{p_1 p_2 r} = z^{\mathfrak{H}} = y, \tag{36}$$

and let us denote for shortness

$$y_1^a y_2^b + y_2^a y_3^b + y_3^a y_1^b = (y_1^a y_2^b),$$
$$y_1^a y_2^b y_3^c + y_2^a y_3^b y_1^c + y_3^a y_1^b y_2^c = (y_1^a y_2^b y_3^c).$$

All invariant forms of $G$ are then given as integral functions of $z_1 z_2 z_3$ and expressions of the form

$$(y_1^{\lambda t+n} . y_2^{\mu t+\nu}). \tag{37}$$

Furthermore, we shall use the following notations:

$$\left.\begin{aligned} y_1 y_2 y_3 &= A, \\ y_1^t + y_2^t + y_3^t &= E. \end{aligned}\right\} \tag{38}$$

If in (37) $n$ runs from 1 to $t-1$, then $n\nu$ will constitute a complete system of residues (mod. $t$). Let us denote

$$n\nu \equiv \nu_n \pmod{t}, \tag{39}$$

where $\nu_n < t$. Then $\nu_n$ will assume all the values from 1 to $t-1$ in some order when $n$ runs from 1 to $t-1$. Thus we obtain $t-1$ forms,

$$(y_1^n y_2^{\nu_n}), \qquad (n = 1, 2, 3, \ldots . t-1),$$

which are contained in (37). We shall denote these special forms by

$$\psi_n = (y_1^n y_2^v), \tag{40}$$

or simply by $\psi$ when no reference to the value of $n$ is needed.

The same system of forms (40) is also, according to (27), given by

$$\psi_{w_n} = (y_1^{w_n} y_2^n), \qquad (n = 1, 2, 3, \ldots . t-1),$$

where again $w_n < t$ is defined by the congruence

$$nw \equiv w_n \pmod t. \tag{41}$$

We now propose to show *that all the invariant forms given by* (37) *are expressible in terms of* $A$, $E$ *and* $\psi_n$.

We know that $v$ will be distinct from $w$ unless $t = 3$. To fix the ideas, let us in the following always assume $v > w$. If in a given case $w$, defined by (24), should be greater than $v$, we have only to interchange $v$ and $w$ or $\alpha$ and $\beta$. We prove now the following lemmas:

1). $y_1 y_2^t + y_2 y_3^t + y_3 y_1^t = (y_1^t y_2^t)$ *is expressible in terms of* $A$, $E$ *and* $\psi$.

From $v^2 \equiv v - 1 \pmod t$

it follows that $v_v = v - 1,$

and likewise $w_w = w - 1.$

Hence $\psi_v = (y_1^v y_2^{v-1})$ and $\psi_w = (y_1^w y_2^{w-1}).$ (42)

Multiplying now $\psi_v . \psi_{w-1}$ we find

$$\psi_v \psi_{w-1} = (y_1^{v+w-1} y_2^{v+w-1}) + A^w (y_1^{v-w} y_2^{v-2}) + A^{w-1} (y_1^{v+1} y_2^{v-w}).$$

But $v + w - 1 = t$, see (31), hence

$$(y_1^t y_2^t) = \psi_v \psi_{w-1} - A^w \psi_{v-w} - A^{w-1} \psi_{v+1}. \tag{43}$$

This deduction fails for $t = 3$. In this case we find directly

$$(y_1^3 y_2^3) = \psi_1 \psi_2 - 3A^2 - AE. \tag{44}$$

2). $(y_1^{t+n} y_2^{v_n})$ *is expressible in terms of* $(y_1^n y_2^{t+v_n})$, $A$, $E$ *and* $\psi$.

This follows immediately by performing the multiplication

$$(y_1^n y_2^{v_n})(y_1^t + y_2^t + y_3^t) = (y_1^{t+n} y_2^{v_n}) + (y_1^n y_2^{t+v_n}) + (y_1^n y_2^{v_n} y_3^t),$$

whence $$(y_1^{t+n} y_2^{v_n}) = -(y_1^n y_2^{t+v_n}) + E . \psi_n - A^n \psi_{v_n - n}, \tag{45}$$

if $n < v_n$. If, however, $n > v_n$, the last term in (45) is to be replaced by $A^{v_n} \psi_{n - v_n}$.

3). $(y_1^{t+n}y_2^{t+v_n})$ *is expressible in terms of* $(y_1^n y_2^{t+v_n})$, $A$, $E$ *and* $\psi$.

We find

$$(y_1^n y_2^{v_n})(y_1^t y_2^t) = (y_1^{t+n}y_2^{t+v_n}) + (y_1^n y_2^{t+v_n} y_3^t) + (y_1^{t+n} y_2^{v_n} y_3^t)$$
$$= (y_1^{t+n}y_2^{t+v_n}) + A^n (y_1^{t+v_n-n}y_2^{t-n}) + A^{v_n}(y_1^{t-v_n}y_2^{t+n-v_n}),$$

or
$$(y_1^{t+n}y_2^{t+v_n}) = E.\psi_n - A^n (y_1^{t+v_n-n}y_2^{t-n}) + A^{v_n}(y_1^{t-v_n}y_2^{t+n-v_n}). \quad (46)$$

If $v_n > n$, then the factor of $A^{v_n}$ in (46) is a function $\psi_n$, and the factor of $A^n$, being of the type $(y_1^{t+m}y_2^{v_m})$, is reducible to $(y_1^m y_2^{t+v_m})$ and $A$, $E$, $\psi_n$, according to (45). If, however, $n > v_n$, then the factor of $A^n$ is a function $\psi_n$ and the factor of $A^{v_n}$ a function $(y_1^n y_2^{t+v_n})$.

4). $(y_1 y_2^{t+v})$ *is expressible in terms of* $A$, $E$ *and* $\psi$.

From
$$(y_1^w y_2)(y_1^v y_2^{v-1}) = (y_1^{t+1}y_2^v) + A(y_1^{v-1}y_2^{t-1}) + A^w (y_1^{v+1-w}y_2^{v-w+1})$$
we obtain
$$(y_1^{t+1}y_2^v) = \psi_w\psi_v - A\psi_{v-1} - A^w p_{v+1-w},$$
and from (45), putting $n = 1$,
$$(y_1^{t+1}y_2^v) = -(y_1 y_2^{t+v}) + E\psi_1 - A\psi_{v-1}.$$
Combining the last two equations, we have
$$(y_1 y_2^{t+v}) = E\psi_1 - \psi_v\psi_w + A^w\psi_{v+1-w}. \quad (47)$$
This deduction fails again for $t = 3$. In this case we find
$$(y_1 y_2^5) = (A + E)\psi_1 - \psi_2^2. \quad (48)$$

5). $(y_1^n y_2^{t+v_n})$ *is expressible in terms of* $A$, $E$ *and* $\psi$.

This theorem has already been proved for $n = 1$ (see lemma 4). In order to prove it for functions $(y_1^{n+1}y_2^{t+v_{n+1}})$ $(n = 1, 2, 3, \ldots . t-2)$, we have to distinguish two cases, viz. $v + v_n = t + v_{n+1}$ and $v + v_n = v_{n+1}$. In the first case let us form the product
$$(y^n y_2^{v_n})(y_1 y_2^v) = (y_1^{n+1}y_2^{t+v_{n+1}}) + A\Psi,$$
whence
$$(y_1^{n+1}y_2^{t+v_{n+1}}) = \psi_1\psi - A\Psi, \quad (49)$$
in the latter,
$$(y_1^n y_2^{v_n})(y_1 y_2^{t+v}) = (y_1^{n+1}y_2^{t+v_{n+1}}) + A\Psi',$$
whence
$$(y_1^{n+1}y_2^{t+v_{n+1}}) = (y_1 y_2^{t+v})\psi_a - A\Psi',$$
or, applying (47),
$$(y_1^{n+1}y_2^{t+v_{n+1}}) = E\psi_1\psi_n - \psi_n\psi_v\psi_w - A\Psi'', \quad (50)$$

where $\Psi$, $\Psi'$ and $\Psi''$ are expressions consisting of functions of the type $(y_1^{t+m}y_2^{t+v_m})$, $(y_1^{t+p}y_2^{v_p})$, $(y_1^n y_2^{t+v_n})$, $E$, $\psi$ and of products of some powers of $A$ into such functions. But $(y_1^{t+m}y_2^{t+v_m})$ and $(y_1^{t+p}y_2^{v_p})$ can be reduced to $A$, $E$, $\psi$, $(y_1^n y_2^{t+v_n})$ according to lemma 2 and 3, and let us suppose that this reduction has actually been made. $\Psi$, $\Psi'$ *and* $\Psi''$ *contain then only functions* $A$, $E$, $\psi$ *and* $(y_1^n y_2^{t+v_n})$. The degrees of all the $t-2$ functions $(y_1^{n+1}y_2^{t+v_{n+1}})$ will be distinct from each other, for any equation

$$n+1+t+v_{n+1}=m+1+t+v_{m+1}$$

would imply $$(n+1)(v+1)\equiv(m+1)(v+1) \pmod t,$$

or $n\equiv m \pmod t$, i. e. $n=m$. (The case $v+1\equiv 0 \pmod t$ leads to $v=t-1$, $w=2$, $t=3$, which shall be excluded.) Let, then, $(y_1^{m+1}y_2^{t+v_{m+1}})$ be that function whose degree is a minimum and now apply formula (49) or (50). The degree of $\Psi$ or of $\Psi''$ is $m+1+t+v_{m+1}-3$. It follows that $\Psi$ and $\Psi''$ cannot contain functions of the type $(y_1^n y_2^{t+v_n})$ at all since $m+1+t+v_{m+1}-3$ is smaller than the smallest possible degree of $(y_1^n y_2^{t+v_n})$. Therefore $(y_1^{m+1}y_2^{t+v_{m+1}})$ must be expressible in terms of $A$, $E$ and $\psi$ only. We now apply the same conclusion to the successive functions $(y_1^{n+1}y_2^{t+v_{n+1}})$ which we arrange according to their dimensions. The functions $\Psi$ and $\Psi''$ occurring in that representation will then contain either no functions $(y_1^n y_2^{t+v_n})$ at all or only those which have already been reduced to $A$, $E$ and $\psi$. Hence we have the theorem: *Every function* $(y_1^n y_2^{t+v_n})$ *is expressible in terms of* $A$, $E$ *and* $\psi$.

The case $t=3$ has again to be treated separately. We find directly

$$(y_1^2 y_2^4)=\psi_1^2-2A\psi_2. \tag{51}$$

Combining now lemmas 1, 2, 3, 4, 5, we have the following result: *The functions* $(y_1^n y_2^{t+v_n})$, $(y_1^{t+n}y_2^{v_n})$, $(y_1^{t+n}y_2^{t+v_n})$ *for all the values of* $n=0, 1, 2, \ldots . t-1$ *are expressible in terms of* $A$, $E$ *and* $\psi$.

Multiplying these functions by $E$ and $y_1^t y_2^t+y_2^t y_3^t+y_3^t y_1^t=B$, we can increase either exponent by $t$. We find

$$(y_1^n y_2^{2t+v_n})=(y_1^n y_2^{t+v_n})E-(y_1^{t+n}y_2^{t+v_n})-A^n(y_1^{t+v_n-n}y_2^{t-n}), \tag{52}$$

and a corresponding formula for $(y_1^{2t+n}y_2^{v_n})$,

$$(y_1^{t+n}y_2^{2t+v_n})=(y_1^n y_2^{t+v_n})B-A^n(y_1^{2t+v_n-n}y_2^{t-n})-A^t\psi_n, \tag{53}$$

and a corresponding formula for $(y_1^{2t+n}y_2^{t+v_n})$,

$$(y_1^{2t+n}y_2^{2t+v_n})=(y_1^{t+n}y_2^{t+v_n})B-A^t(y_1^n y_2^{t+v_n})-A^t(y_1^{t+n}y_2^{v_n}). \tag{54}$$

This method can be continued until all the functions $(y_1^{\lambda t+n} y_2^{\mu t+\nu_n})$, where $\lambda, \mu = 0, 1, 2, 3, \ldots$ and $n = 1, 2, 3, \ldots t-1$, are expressed in terms of $A$, $B$, $E$ and $\psi$, i. e. in terms of $A$, $E$ and $\psi$, since $B$ itself is given in terms of $A$, $E$ and $\psi$, see (43) and (44).

The case $n = 0$ requires a special deduction. If $\lambda = \mu$, then the function $(y_1^{\lambda t} y_2^{\lambda t})$ is symmetrical, and therefore expressible in terms of

$$\begin{aligned} y_1^t + y_2^t \quad + y_3^t &= E, \\ y_1^t y_2^t + y_2^t y_3^t + y_3^t y_1^t &= B, \\ y_1^t y_2^t y_3^t &= A^t. \end{aligned}$$

If $\lambda \neq \mu$ it becomes necessary to express the product of differences,

$$(y_1^t - y_2^t)(y_2^t - y_3^t)(y_3^t - y_1^t) = (y_1^t y_2^{2t}) - (y_1^{2t} y_2^t).$$

We obtain this by performing the multiplications

$$(y_1^v y_2^{t+v-1}).(y_1^{w-1} y_2^w) \text{ and } (y_1^{t+w-1} y_2^w)(y_1^v y_2^{v-1}).$$

The result is:

$$(y_1^t y_2^{2t}) = \psi_{w-1}(y_1^v y_2^{t+v-1}) - A^w (y_1^{v-w} y_2^{t+v-2}) - A^{w-1}(y_1^{v+1} y_2^{t+v-w}), \quad (55)$$

$$(y_1^{2t} y_2^t) = \psi_v (y_1^{t+w-1} y_2^w) \quad - A^w (y_1^{v-w} y_2^{t+v-2}) - A^{v-1}(y_1^{t+w-v} y_2^{w+1}). \quad (56)$$

Now, every function $(y_1^{\lambda t} y_2^{\mu t})$ is expressible in terms of the symmetric functions $A$, $B$, $E$ and of (55) and (56).

Thus we have the final result:

*Denote* $r_1 r_2 p = \mathfrak{H}$, $y = z^\vartheta$, $y_1 y_2 y_3 = A$, $y_1^t + y_2^t + y_3^t = E$, $(y_1^n y_2^{\nu_n}) = \psi_n$, *and suppose* $t > 1$, *then every invariant form of* $G$ *is an integral function of* $z_1 z_2 z_3 = \sqrt[\vartheta]{A}$, $E$ and $\psi_n$ $(n = 1, 2, \ldots t-1)$.

This system of the $t+1$ forms $\sqrt[\vartheta]{A}$, $E$, $\psi_n$ may be called the "*reduced system*" of invariant forms. It is in general greater than the "*complete system*,"* and it contains the forms of the complete system. The results of the next section will show that for $t > 3$ some of the forms $\psi_n$ can be expressed as integral functions of the other forms of the reduced system.

---

* A complete system of invariant forms is given by the *minimum* number of invariants such that every other invariant may be expressed as an integral function of the forms of the system.

## §4. *Special Cases.*

### I. $t = 1$.

The case $t = 1$ covers a great many special groups $G$; for instance, all those where $R$, the greatest common divisor of $m_1$ and $m_2$, is either 1, or where it consists of prime factors of the form $3h + 2$, i. e. 2, 5, 11, etc.

For $t = 1$ the formulæ (26) are reduced to

$$\alpha = \lambda\vartheta \text{ and } \beta = \mu\vartheta,$$

where $\lambda$ and $\mu$ are two integers. All invariant forms are therefore given by $z_1 z_2 z_3$ and $(z_1^{\lambda\vartheta} z_2^{\mu\vartheta})$; they are expressible as integral functions of

$$z_1 z_2 z_3 = \sqrt[\vartheta]{A},$$
$$y_1 + y_2 + y_3 = E,$$
$$y_1 y_2 + y_2 y_3 + y_3 y_1 = B,$$

and
$$(y_1 - y_2)(y_2 - y_3)(y_3 - y_1) = \Delta.$$

*These four forms constitute therefore the complete system of invariants of the group.* There exists one relation between them, viz.

$$\Delta^2 = 18ABE - 4AE^3 - 4B^3 + B^2E^2 - 27A^2.$$

### II. $t = 3$.

In this case the reduced system consists of

$$\sqrt[\vartheta]{A},\ E,\ \psi_1 = (y_1 y_2^2),\ \psi_2 = (y_1^2 y_2),$$

which is also the complete system. The relation between its four forms is this:

$$\psi_1^3 + \psi_2^3 - \psi_1\psi_2(6A + E) + A(9A^2 + 3AE + E^2) = 0.$$

### III. $t = 7$.

The roots of the congruence

$$\omega^2 - \omega + 1 \equiv 0 \pmod 7$$

are $v = 5$, $w = 3$. The reduced system consists of

$$\sqrt[\vartheta]{A},\ E \text{ and 6 functions } \psi_n = (y_1^n y_2^{v_n}) \quad (n = 1, 2, \ldots 6).$$

Corresponding values of $n$ and $v_n$ are given in the following table:

| $n =$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $v_n =$ | 5 | 3 | 1 | 6 | 4 | 2 |

The complete system consists of $\sqrt[3]{A}$, $E$, and $\psi_1, \psi_2, \psi_3$. We find

$$\psi_4 = \psi_2^2 - 2A^2\psi_3,$$
$$\psi_5 = \psi_2\psi_3 - A\psi_1 - 3A^3,$$
$$\psi_6 = \psi_3^2 - 2A\psi_2.$$

There must exist two relations between the five forms of the complete system. These are

$$\left.\begin{aligned} &\psi_2^2 - \psi_1\psi_3 + AE - A^2\psi_3 = 0, \\ &\psi_1^2 + \psi_3^2 - E\psi_2 - 5A\psi_2\psi_3 + 3A^2\psi_1 + 9A^4 = 0. \end{aligned}\right\} \tag{57}$$

As an example may serve the group* generated by

$$S: \begin{aligned} z_1' &= z_2, \\ z_2' &= z_3, \\ z_3' &= z_1, \end{aligned} \quad \text{and} \quad T: \begin{aligned} z_1' &= \gamma z_1, \\ z_2' &= \gamma^4 z_2, \\ z_3' &= \gamma^2 z_3, \end{aligned} \quad \text{where } \gamma = e^{\frac{2\pi i}{7}}.$$

We have here $m_1 = m_2 = 7$; hence $R = 7$, $p_1 = p_2 = 1$, $k_1 = 1$, $k_2 = 4$ and also $\varkappa_1 = 1$, $\varkappa_2 = 4$; $p = \varkappa_1 p_2 = 1$, $q = \varkappa_2 p_1 = 4$, $p^2 + pq + q^2 = 21$, therefore $t = 7$, $r = 1$, $\mathfrak{d} = p_1 p_2 r = 1$. The congruence $4v \equiv -1 \pmod 7$ gives $v = 5$. The complete system is therefore given by

$$\left.\begin{aligned} A &= z_1 z_2 z_3 \qquad\qquad\quad , \\ \psi_3 &= z_1^3 z_2 + z_2^3 z_3 + z_3^3 z_1, \\ \psi_2 &= z_1^2 z_2^3 + z_2^2 z_3^3 + z_3^2 z_1^3, \\ \psi_1 &= z_1 z_2^5 + z_2 z_3^5 + z_3 z_1^5, \\ E &= z_1^7 \quad + z_2^7 \quad + z_3^7 \quad . \end{aligned}\right\} \tag{58}$$

## IV. $t = 13$.

The roots of the congruence

$$\omega^2 - \omega + 1 \equiv 0 \pmod{13}$$

are $v = 10$, $w = 4$. The reduced system consists of

$$\sqrt[3]{A},\ E,\ \text{and 12 functions } \psi_n = (y_1^n y_2^{v_n}) \qquad (n = 1, 2, \ldots . 12).$$

---

* This group (of order 21) and its invariant forms play an important part in many investigations. The group occurs as a subgroup of the $G_{168}$ mentioned in the introduction, and also as a subgroup of a quaternary $G_{168}$ (see my paper on this group read at the International Mathematical Congress, Chicago, 1893), which latter is contained again as a subgroup in a quaternary group of order $\frac{7!}{2}$ (F. Klein, Ueber Gleichungen 6. und 7. Grades, Math. Ann., Bd. 28, p. 517). Klein's investigations on transformation of the 7th order (Math. Ann., Bd. 13, p. 428) are based on the curve $\psi_3 = z_1^3 z_2 + z_2^3 z_3 + z_3^3 z_1 = 0$ (see also Haskell, *American Journal,* Vol. XIII, p. 1). The five invariants (58) and the two syzygies (57) occur also in a paper by Brioschi, "Ueber die Jacobischen Modulargleichungen vom 8ten Grad" (Math. Ann., Bd. 15, p. 241).

The corresponding values of $n$ and $v_n$ are these:

| $n =$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $v_n =$ | 10 | 7 | 4 | 1 | 11 | 8 | 5 | 2 | 12 | 9 | 6 | 3 |

The complete system consists of $\sqrt[3]{A}$, $E$, $\psi_1$, $\psi_2$, $\psi_3$, $\psi_4$. We find

$$\begin{aligned}
\psi_5 &= \psi_2\psi_3 - A^2\psi_4^2 + A^3\psi_3,\\
\psi_6 &= \psi_3^2 - 2A^3\psi_4,\\
\psi_7 &= \psi_3\psi_4 - A\psi_2 - 3A^4,\\
\psi_8 &= \psi_4^2 - 2A\psi_3,\\
\psi_9 &= \psi_3^3 - 3A^3\psi_3\psi_4 + 3A^7,\\
\psi_{10} &= \psi_3^2\psi_4 - A\psi_2\psi_3 - A^3\psi_4^2 - 2A^4\psi_3,\\
\psi_{11} &= \psi_3\psi_4^2 - A(\psi_2\psi_4 + \psi_3^2) - 2A^4\psi_4,\\
\psi_{12} &= \psi_4^3 - 3A\psi_3\psi_4 + 3A^5.
\end{aligned}$$

The three relations between the six forms of the complete system are

$$\begin{aligned}
\psi_2^2 &= \psi_1\psi_3 - A\psi_4^3 + 5A^2\psi_3\psi_4 - 3A^3\psi_2 - 9A^6,\\
\psi_3^2 &= \psi_2\psi_4 - A\psi_1 + A^3\psi_4,\\
\psi_1\psi_4 - \psi_2\psi_3 &= AE - A^3\psi_3.
\end{aligned}$$

## V. $t = 19$.

The solutions of the congruence

$$\omega^2 - \omega + 1 \equiv 0 \pmod{19}$$

are $v = 12$, $w = 8$. The reduced system consists of

$\sqrt[3]{A}$, $E$ and 18 functions $\psi_n = (y_1^n y_2^{v_n})$ $\quad (n = 1, 2, \ldots . 18)$.

Corresponding values of $n$ and $v_n$ are

| $n =$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $v_n =$ | 12 | 5 | 17 | 10 | 3 | 15 | 8 | 1 | 13 | 6 | 18 | 11 | 4 | 16 | 9 | 2 | 14 | 7 |

The complete system consists of $\sqrt[3]{A}$, $E$, $\psi_1$, $\psi_2$, $\psi_5$, $\psi_8$.

We find

$$\begin{aligned}
\psi_3 &= \psi_1\psi_2 - A\psi_5\psi_8 + A^4\psi_5,\\
\psi_4 &= \psi_2^2 - 2A^2\psi_5,\\
\psi_6 &= \psi_2^3 - 3A^2\psi_2\psi_5 + 3A^7,\\
\psi_7 &= \psi_2\psi_5 - A^2\psi_8 - 3A^5,\\
\psi_9 &= \psi_2^2\psi_5 - 2A^2\psi_5^2 - A^3\psi_1 - A^5\psi_2,
\end{aligned}$$

$$\psi_{10} = \psi_2\psi_8 - A\psi_1 - A^3\psi_2,$$
$$\psi_{11} = \psi_2^3\psi_5 - A^2\psi_2(2\psi_5^2 + \psi_2\psi_8) + A^4\psi_5\psi_8 - 2A^5\psi_2^2 + 4A^7\psi_5,$$
$$\psi_{12} = \psi_2^2\psi_8 - A\psi_1\psi_2 - A^2\psi_5\psi_8 - 2A^5\psi_5,$$
$$\psi_{13} = \psi_5\psi_8 - A\psi_2^2 + A^3\psi_5,$$
$$\psi_{14} = \psi_2^2\psi_5^2 - 2A^2\psi_2\psi_5\psi_8 + A^4\psi_8^2 - 6A^5\psi_2\psi_5 + 4A^7\psi_8 + 9A^{10},$$
$$\psi_{15} = \psi_2\psi_5\psi_8 - A\psi_2^3 - A^2\psi_2^2\psi_8 + 3A^3\psi_2\psi_5 - 3A^5\psi_8 - 6A^8,$$
$$\psi_{16} = \psi_8^2 - 2A\psi_2\psi_5 + 2A^3\psi_8 + 6A^6,$$
$$\psi_{17} = \psi_2^2\psi_5\psi_8 - A\psi_1\psi_2\psi_5 - A^2\psi_2\psi_8^2 + A^3(\psi_1\psi_8 - \psi_2^2\psi_5) - 2A^5\psi_2\psi_8 + 2A^6\psi_1 + 2A^8\psi_2,$$
$$\psi_{18} = \psi_2\psi_8^2 - A(\psi_1\psi_8 + \psi_2^2\psi_5) + A^3(2\psi_5^2 - \psi_2\psi_8) + A^4\psi_1.$$

The three relations between the six forms of the complete system are

$$\psi_1^2 = E\psi_2 - \psi_5\psi_8^2 + 4A\psi_2\psi_5^2 - 3A^3\psi_5\psi_8 - 3A^4\psi_2^2 - 9A^6\psi_5,$$
$$\psi_2^3 = \psi_1\psi_5 - A\psi_8^2 + 5A^2\psi_2\psi_5 - 3A^4\psi_8 - 9A^7,$$
$$\psi_5^2 = \psi_2\psi_8 - A\psi_1 + A^3\psi_2.$$

## §5. *Order and Subgroups of G.*

Let us consider the three substitutions

$$T,\ STS^{-1} = U,\ \text{and}\ S^{-1}TS = V,$$

where $S$ and $T$ are the two generating substitutions of $G$ given in (1) and (2):

$$\left.\begin{aligned} z_1' &= a_1z_1 \\ z_2' &= a_2z_2 \\ z_3' &= a_3z_3 \end{aligned}\right\} = T, \qquad \left.\begin{aligned} z_1' &= a_2z_1 \\ z_2' &= a_3z_2 \\ z_3' &= a_1z_3 \end{aligned}\right\} = U, \qquad \left.\begin{aligned} z_1' &= a_3z_1 \\ z_2' &= a_1z_2 \\ z_3' &= a_2z_3 \end{aligned}\right\} = V,$$

and let us find all those substitutions $R$ which are generated by $T$, $U$ and $V$. It is obvious that *they are all interchangeable.* On account of $a_1a_2a_3 = 1$ we have $V = (TU)^{-1}$, therefore we may confine ourselves to $T$ and $U$. The general form of all possible substitutions $R$ generated by $T$ and $U$ is $T^mU^n$, and since $P$ is the period of $T$ and of $U$, the substitutions $R$ are given by this table:

$$\left.\begin{array}{llll} 1 & , T & , T^2 & \ldots . T^{P-1} \\ U & , TU & , T^2U & \ldots . T^{P-1}U \\ U^2 & , TU^2 & , T^2U^2 & \ldots . T^{P-1}U^2 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ U^{P-1}, & TU^{P-1}, & T^2U^{P-1} & \ldots . T^{P-1}U^{P-1}. \end{array}\right\} \qquad (59)$$

Now it may happen that some power of $T$ will be equal to some power of $U$. The condition for $T^\lambda = U^\mu$ is:

$$a_1^\lambda = a_2^\mu,\ a_2^\lambda = a_3^\mu,\ a_3^\lambda = a_1^\mu \qquad (60)$$

or, see (3),

$$\frac{\lambda k_1}{m_1} - \frac{\mu k_2}{m_2} = \lambda_1,$$
$$\frac{\lambda k_2}{m_2} - \frac{\mu k_3}{m_3} = \lambda_2,$$
$$\frac{\lambda k_3}{m_3} - \frac{\mu k_1}{m_1} = \lambda_3,$$

where $\lambda_1$, $\lambda_2$, $\lambda_3$ are three integers. But these three equations coincide exactly with the equations (7) which have already been solved in §1. The solutions of our equations (60) are, therefore, see (26): $\lambda = \alpha$, $\mu = -\beta$, or in full length:

$$\lambda = p_1 p_2 r\,(lt + n),$$
$$\mu = -p_1 p_2 r\,(mt + nv).$$

The smallest power $\lambda$ satisfying the equation $T^\lambda = U^\mu$ is therefore

$$\lambda = p_1 p_2 r = \mathfrak{S},$$

and the corresponding power $\mu = \mathfrak{S}\,(t - v)$; but $v + w - 1 = t$, hence $t - v = w - 1$. We have, therefore,

$$T^{\mathfrak{S}} = U^{\mathfrak{S}(w-1)},$$

and likewise

$$U^{\mathfrak{S}} = T^{\mathfrak{S}(v-1)}.$$

The consequence is that only the substitutions of the first $\mathfrak{S} - 1$ rows of table (59) will be all distinct from each other, while the remaining substitutions will be equal to some substitutions of the first $\mathfrak{S} - 1$ rows. We have then altogether $\mathfrak{S}.P$ distinct substitutions $R$. But every substitution of $G$ can be thrown into the form $R$, $RS$ or $RS^2$, because $SRS^{-1}$ is again one of the substitutions $R$, say $R'$, so that $SR = R'S$. $G$ contains, therefore, $3\mathfrak{S}P$ substitutions. Thus we have the result:

*The order of* $G$ *is* $3\mathfrak{S}P = 3\mathfrak{S}^2 t = 3p_1^2 p_2^2 r^2 t$.

If $t = 1$, we have $\mathfrak{S} = P$, and the order of $G = 3P^2$; in this case the $P^2$ substitutions of table (59) are all distinct. If $\mathfrak{S} = 1$, we have $t = P$ and the order of $G = 3P$ so that the distinct substitutions $R$ will be given by the first row of table (59).

In every case the substitutions $R$ form a *self-conjugate subgroup* $H$ within $G$ of order $\mathfrak{S}P = \mathfrak{S}^2 t$. But there exists another self-conjugate subgroup $H'$ of order $t$. This is formed by the $t$ powers of $T^{\mathfrak{S}}$, for there is

$$ST^{\mathfrak{S}}S^{-1} = U^{\mathfrak{S}} = T^{\mathfrak{S}(v-1)},$$

and

$$RT^{\mathfrak{S}}R^{-1} = T^{\mathfrak{S}}.$$

Evidently $H'$ is contained in $H$. If $\mathfrak{S} = 1$, $H'$ coincides with $H$, and if $t = 1$, $H'$ is reduced to unity.

UNIVERSITY OF CHICAGO, *December* 24, 1894.